What is claimed is:

1. A content information distribution apparatus for distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising:

(a) a unit (302) for encrypting content information encoded by a prescribed encoding system;

(b) a unit (304) for generating an encryption attribute header including attribute information with regard to the encryption of the content information;

(c) a unit (306) for performing transport protocol processing required to transfer the content information and for generating a basic transport header to be added to the content information to which the encryption attribute header has been added; and

(d) a unit (for sending to the other end apparatus that is authenticated a packet including the basic transport header, the encryption attribute header, and the encrypted content information, wherein the encryption attribute header is set into an expansion transport header within a packet header of the packet or into a payload header within a payload to be encrypted of the packet.

2. The apparatus according to claim 1, wherein the encryption attribute header includes at least one of the existence or non-existence of encryption of the content information and the encryption system of the content information.

3. The apparatus according to claim 1, wherein the encryption attribute header includes a copy attribute field having a plurality of bits with regard to the number of copying of the content information.

4. The apparatus according to claim 1, wherein the encryption attribute header includes a counter field indicating a change in

an encryption key.

5. The apparatus according to claim 1, wherein the unit (b) sets the encoding information, which indicates the encoding system for the content information into the expansion transport header or into the payload header.

6. The apparatus according to claim 1, wherein the unit (c) further codes into the basic transport header at least information indicating that there is a possibility that the content information is encrypted, and wherein the unit (b) codes into the expansion header at least information as to whether or not the content information to be transferred is encrypted.

7. The apparatus according to claim 1, wherein the unit (b) codes into the expansion header information as to whether or not the content information to be transferred is encrypted.

8. The apparatus according to claim 1, further comprising:

(e) a unit for generating a content attribute header that includes content attribute information with regard to content information, and for setting this content attribute header into the expansion transport header or into the payload header.

9. The apparatus according to claim 8, wherein the content attribute header is not encrypted.

10. The apparatus according to claim 1, wherein the unit (a) generates the encryption key based on an identifier that uniquely identifies a storage medium sent from the other end apparatus in a communication.

11. A content information receiving apparatus authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure and which receives encrypted content information via a network in accordance

with a prescribed transport protocol, comprising:

(aa) a unit for receiving from a sending apparatus a packet containing a basic transport header, an encryption attribute header including attribute information with regard to the encryption of the content information, and encrypted content information;

(bb) a unit for referring to the basic transport header or encryption attribute header and judging whether or not the content information is encrypted or whether there is a possibility that the content information is encrypted; and

(cc) a unit that, when a judgment is made by the unit (bb) that the content information is encrypted, decrypts the encrypted content information, based on the attribute information with regard to encryption included in the encryption attribute header.

12. The apparatus according to claim 11, wherein the unit (bb), when there is a possibility that the content information is encrypted, refers to the encryption attribute header and judges whether or not the content information is encrypted.

13. The apparatus according to claim 11, wherein the unit (bb) refers to the basic transport header or to the encryption attribute header to make a judgment as to the encoding system of the content information.

14. The apparatus according to claim 11, further comprising:

(dd) a unit for referring to a received basic transport header and, when a prescribed delay time has elapsed or a prescribed number of packets have been discarded, requesting that the sending apparatus send a prescribed encryption parameter.

15. A method of distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(a) encrypting content information encoded by a prescribed encoding system;

(b) adding an encryption attribute header including attribute information with regard to the encryption of the content information to the encrypted content information;

(c) adding a content attribute header indicating attributes of the content information to content information to which the encryption attribute header has been added;

(d) performing transport protocol processing required to transfer the content information, and adding a basic transport header to content information to which the content attribute header has been added; and

(e) sending a packet including the basic transport header, the encryption attribute header, the content attribute header, and the encrypted content information to the other end authenticated apparatus,

wherein the encryption attribute header is set into either an expansion transport header within a packet header of the packet, or into a payload header within an encrypted payload of the packet.

16. A method of distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(a') adding a content attribute header indicating attributes of the content information to the content information to be transferred;

(b') encrypting content information that are encoded by a prescribed encoding system and to which the content attribute header has been added;

(c') adding to the encrypted content information an encryption attribute header including attribution information with regard to the encryption of the content information;

(d') performing transport protocol processing required to

transfer the content information, and adding a basic transport header to content information to which the encryption attribute header has been added; and

(e') sending a packet including the basic transport header, the encryption attribute header, the content attribute header, and the encrypted content information to the other end authenticated apparatus,

wherein the encryption attribute header is set into either an expansion transport header within a packet header of the packet, or into a payload header within a payload to be encrypted of the packet.

17. A method of receiving encrypted content information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(aa) receiving a packet including a basic transport header, an encryption attribute header including encryption attribute information with regard to the encryption of the content information, and encrypted content information;

(bb) referring to the basic transport header and judging whether or not the content information is encrypted or whether or not there is a possibility that the content information is encrypted;

(cc) referring to the encryption attribute header and extracting encryption attribute information with regard to encryption of the content information;

(dd) referring to an expansion transport header within a packet header of the packet and extracting content attribute information with regard to the content information; and

(ee) in the case in which a judgment is made at (bb) that the content information is encrypted, decrypting the encrypted content information, based on the extracted encryption attribute information.

18. A method of receiving encrypted content information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(aa') receiving a packet including a basic transport header, an encryption attribute header including encryption attribute information with regard to the encryption of the content information, and encrypted content information;

(bb') referring to the basic transport header and judging whether or not the content information is encrypted or whether or not there is a possibility that the content information is encrypted;

(cc') in the case in which a judgment is made at (bb') that the content information is encrypted, referring to the encryption attribute header and extracting encryption attribute information with regard to the encryption of the content information;

(dd') in the case in which a judgment is made at (bb') that the content information is encrypted, decrypting the encrypted content information based on the extracted encryption attribute information; and

(ee') referring to an expansion transport header within a packet header of the packet and extracting content attribute information with regard to the content information.

19. A computer-readable recording medium for recording a program to be executed by a computer, the program performing distribution of encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, the program comprising:

(a) a module for generating an encryption attribute header including attribute information with regard to encryption of the content information;

(b) a module for performing transport protocol processing

required to transfer the content information and for generating a basic transport header to be added to the content information to which the encryption attribute header has been added; and

(c) a module for sending a packet including the basic transport header, the encryption attribute header, and the encrypted content information to the other end authenticated apparatus,

wherein the encryption attribute header is set either into an expansion transport header within a packet header of the packet or into a payload header within a payload to be encrypted of the packet.

20. A computer-readable recording medium for recording a program to be executed by a computer, the program performing receiving of encrypted content information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, the program comprising:

(aa) a module for receiving from a sending apparatus a packet including a basic transport header, an encryption attribute header including attribute information with regard to encryption of the content information, and encrypted content information;

(bb) a module for referring to the basic transport header or the encryption attribute header and judging whether or not the content information is encrypted or whether there is a possibility that the content information is encrypted; and

(cc) a module for decrypting the encrypted content information based on attribute information with regard to encryption included in the encryption attribute header, in the case in which a judgment is made by module (bb) that the content information is encrypted.